CLAIMS

1. A cryptographic system combining the so-called discrete logarithm and factorization principles, comprising, among other things, public keys and a secret key, characterised in that the said public keys comprise, at least:

a. an RSA modulus n, greater in size than 640 bits, having the following property:

$$n = (A\ p_A + 1) \times (B\ p_B + 1)$$

in which:

p_A and p_B are prime numbers greater in size than 320 bits,

$(A\ p_A + 1)$ is an RSA prime denoted p,

$(B\ p_B + 1)$ is an RSA prime denoted q,

A is the product of k/2 (k being an even integer number between 10 and 120) prime numbers (denoted p[i], i = 1 to k/2) of relatively small size (between 2 and 16 bits) and

B is the product of k/2 prime numbers (also denoted p[i], i = k/2 + 1 to k);

the p[i]s being of relatively small size (between 2 and 16 bits), and also able to be mutually prime;

b. an exponentiation base g, of order $\phi(n)/4$ (where $\phi(n)$ denotes the Euler indicator function), g therefore having not to be a p[i]-th power modulo n of any number.

2. A cryptographic system according to Claim 1 comprising at least an encryption/decryption system 1, characterised in that the encryption of a message m, $m < AB$, consists of the operation:

$$c = g^m \bmod n$$

where c denotes the cryptogram (encrypted message).

3. A cryptographic system according to Claim 2 comprising an encryption/decryption system, characterised in that the integrity of m can be provided by the encryption of m|h(m) (h denoting a hashing function and | denoting concatenation), or by the encryption of DES(key, m), the said key being a key accessible to all.

4. A cryptographic system according to Claim 1 comprising an encryption/decryption system and a key escrow system, characterised in that:

the said secret key of the decrypter or of the escrow centre is the number $\phi(n)$, and in that the operation of decryption or of recovering the identity of a user consists of the following steps:

a. calculating, for i from 1 to k: $y[i] = c^{\phi(n)/p[i]} \bmod n$;

b. for i from 1 to k
for j from 1 to p[i]
comparing y[i] with the values $g^{j\phi(n)/p[i]} \bmod n$ independent of m;
if $g^{j\phi(n)/p[i]} \bmod n = y[i]$ then assign $\mu[i] = j$

c. reconstructing the message m from the Chinese remainder theorem CRT and the values $\mu[i]$.

5. A cryptographic system according to Claim 4 or 5 comprising an encryption/decryption system and a key escrow system, characterised in that the said decrypter speeds up the calculation of the quantities y[i] by calculating:

a) $z = c^r \bmod n$ where $r = p_A p_B$

b) for i from 1 to k: $y[i] = z^{AB/p[i]} \bmod n$,

so as to take advantage of the difference in size between AB/p[i] and $\phi(n)/p[i]$ for speeding up the calculations.

6. A cryptographic system according to Claim 4 comprising an encryption/decryption system and a key escrow system or 5, characterised in that the decrypter pre-calculates and saves, once and for all, the table of values $g^{j\phi(n)/p[i]} \bmod n$ for $1 \leq i \leq k$ and $1 \leq j \leq p[i]$

or,

more specifically, a truncation or a hashing of these values (denoted h) having the following property:

$$h(g^{j\phi(n)/p[i]} \bmod n) \neq h(g^{j'\phi(n)/p[i]} \bmod n) \text{ if } j \neq j'.$$

7. A cryptographic system according to any one of Claim 4 to 6 comprising an encryption/decryption system and a key escrow system, characterised in that the decrypter speeds up its calculations by separately decrypting the message modulo p and then modulo q, and constructing the modulo results with the help of the Chinese remainder theorem in order to find m again.

8. A cryptographic system according to any one of Claims 4 to 7, characterised in that a key escrow centre or authority implements the following steps:

a. it codes the identity of the user $ID = \Sigma\ 2^{i-1}\ ID[i]$ where ID[i] are the bits of the identity of the said user of the system (the sum being taken for i from 1 to k) by calculating $e(ID) = \Pi\ p[i]^{ID[i]}$ (the product being taken for i from 1 to k);

b. it issues, to the user, an El-Gamal key (that is to say an exponentiation base) $c = g^{e(ID)u} \bmod n$,

in which u is a large random prime or a number prime with $\phi(n)$;

c. it thus makes it possible for the user to derive, from c, his El-Gamal public key by choosing a random number x and raising c to the power x modulo n.

d. with the aim of finding the trace of the user, the authority extracts, from the El-Gamal cryptogram of the encrypter, the said cryptogram always comprising two parts, the part:

$$v \equiv c^r \bmod n$$

where r is the encryption random number chosen by the encrypter.

e. Knowing $\phi(n)$, the said authority finds the bits ID[i] by means of the following algorithm:

1. calculate, for i from 1 to k: $y[i] = v^{\phi(n)/p[i]} \bmod n$

2. if y[i] = 1, then $\mu[i] = 1$, otherwise $\mu[i] = 0$

3. calculate:

$$ID' = \Sigma\ 2^{i-1}\ \mu[i]$$

4. find : ID = CCE(ID')

in which CCE denotes an error correction mechanism.

9. A cryptographic system according to any one of Claims 4 to 7 comprising a key escrow system, characterised in that it is based on the so-called Diffie-Hellman key exchange mechanism where a number c, obtained by raising g to a random power a modulo n by one of the parties, is intercepted by the said escrow authority:

$$c = g^a \bmod n$$

the said escrow authority finds a again in the following manner:

a. knowing the factorization of n, the said authority finds, with the help of the decryption algorithm, the value

$$\alpha = a \bmod AB$$

that is $a = \alpha + \beta AB$;

b. the said authority calculates: $\lambda = c/g^{\alpha} \bmod n = g^{\beta AB} \bmod n$

c. using a cryptanalysis algorithm, the authority calculates the discrete logarithm β

$$\lambda = (g^{AB})^{\beta} \bmod n$$

d. the authority finds

$$a = \alpha + \beta AB$$

and decrypts the communications based on the use of a.

10. A cryptographic system according to any one of Claims 2 to 9 comprising an encryption/decryption system and a key escrow system, characterised in that the RSA modulus n is the product of three factors:

$$n = (Ap_A + 1) \times (Bp_B + 1) \times (Cp_C + 1)$$

in which P_A, P_B, P_C are prime numbers greater in size than 320 bits,

$(Ap_A + 1)$, $(Bp_B + 1)$, $(Cp_C + 1)$ are RSA primes, denoted respectively p, q, r,

A, B and C are each the product of k/3 prime numbers (denoted p[i], i = 1 to k), the p[i]s being of relatively small size (between 2 and 16 bits) and able to be mutually prime numbers and k being an integer number between 10 and 120, so that the product ABC has at least 160 bits.

11. A cryptographic system according to any one of Claims 1 to 10 comprising an encryption/decryption or escrow system, characterised in that the items of encryption, decryption and key escrow equipment are computers, chip cards, PCMCIA cards, badges, contactless cards or any other portable equipment.

12. A device comprising a cryptographic system according to any one of the preceding claims, characterised in that it comprises an encryption

system and/or a decryption system and/or a key escrow system, the said systems communicating with one another by an exchange of electronic signals or by means of an exchange of radio waves or infrared signals.